UNITED STATES OF AMERICA	)	
	)	**STIPULATION OF**
v.	)	**EXPECTED TESTIMONY**
	)	
Manning, Bradley E.	)	**SA Calder Robertson**
PFC, U.S. Army,	)	
HHC, U.S. Army Garrison,	)	
Joint Base Myer-Henderson Hall	)	**DATED: 3 June 2013**
Fort Myer, Virginia 22211	)	

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if Special Agent Calder Robertson were present to testify during the merits and pre-sentencing phases of this court martial, he would testify substantially as follows:

1. I am a Special Agent (SA) for the Computer Crime Investigative Unit (CCIU) of the U.S. Army Criminal Investigation Command (CID). I have been with CCIU since March 2006. In February 2010, I became the Special Agent-in-Charge (SAC) of the Europe Branch Office of CCIU. In my current capacity, I am responsible for conducting and overseeing the conduct of large-scale complex criminal investigations associated with high technology, including insider threat and computer intrusions into the critical information architecture of the U.S. Army. Among other things, this work includes: conducting interviews, executing search warrants, processing crime scenes, collecting and handling physical evidence, obtaining forensic images of digital evidence, conducting forensic examinations, and preparing comprehensive reports for supported officials and prosecutors. I have testified several times in judicial proceedings. Because I am in charge of the Europe Branch Office of CCIU, I have responsibility for investigating cyber crime incidents in Europe and Africa, as well as providing rapid response to Southwest Asia (Iraq and Afghanistan). Additionally, I was recently selected to establish the Pacific Branch Office of CCIU, with responsibility for investigating U.S. Army cyber crime incidents in the Pacific area of operations. From April 1998 to November 2003, I held a variety of other positions within CID and was responsible for investigating criminal offenses with an Army nexus.

2. I received a B.S. in Psychology in 2006 and have been a Certified Computer Crime Investigator through the Defense Cyber Crime Center (DC3) since 2007. In 2010, I was awarded the U.S. Army Achievement Medal for Distinguished Civilian Service as a civilian Special Agent for Army CID. I have received numerous other awards in my civilian and military capacities.

3. I have received extensive training from the Defense Cyber Investigations Training Academy (DCITA), which is part of DC3. Through DCITA, I have attended the following courses relevant to my current work: Live Network Investigations (2009), Mobile Electronics Forensics Training (2008), Advanced Log Analysis (2008), Forensics and Intrusions in a Windows Environment (2007), Macintosh Forensic Examinations (2007), Wireless Technology (2007), Windows Forensic Examinations with EnCase (2007), Introduction to Networks and Computer Hardware (2006), and Introduction to Computer Search and Seizure (1999). Additionally, I attended Computer Forensics II with EnCase in 2009, a course put on by Guidance Software, the

PROSECUTION EXHIBIT 23 for identification
PAGE OFFERED:____ PAGE ADMITTED:____
PAGE____OF____PAGES

makers of EnCase. In 2011, I also attended DCITA's Large Data Set Acquisition course as well as the Army Criminal Investigation Laboratory's Evidence Management Certification Course. These courses focused on the collection and handling of physical and digital evidence.

4. On 27 May 2010, I became involved with the investigation of PFC Bradley Manning after receiving preliminary information on misconduct that required downrange investigation. As the SAC of the Europe Branch Office of CCIU and the closest CCIU agent to Iraq, I was tasked by CCIU Headquarters, then at Fort Belvoir, Virginia, to provide support to the Camp Liberty CID office. I traveled to Camp Liberty in Baghdad and stayed there for three days at the end of May 2010. I stayed at Camp Liberty because, at that time, it was too dangerous to travel to FOB Hammer. Additionally, the evidence collection team already at the crime scene on FOB Hammer had sufficient personnel to complete their mission such that my physical presence was unnecessary. My role in the investigation was to assess and provide expert assistance with the collection, preservation, and imaging of computer evidence as well as to perform preliminary analysis of the digital evidence. A preliminary forensic examination is a brief review taking no more than a couple of hours, whereas a full forensic examination may take anywhere from an entire day to several weeks, depending on the amount of recoverable information. I conducted preliminary forensic examinations on a number of items of evidence seized in this case. Evidence collected from FOB Hammer and delivered to me at Camp Liberty included: two Supply Annex computers, a rewriteable CD, an Apple brand personal laptop, an external hard disk drive, and three Sensitive Compartmented Information Facility (SCIF) computers.

5. I follow several general procedures when handling evidence. I review the custody document and always ensure the description of the evidence matches the evidence attached. I check, for example, that recorded serial numbers, markings for identification, and condition description match the associated evidence. I ensure that the necessary information, such as date and time, are properly and accurately recorded. Lastly, I maintain secure custody of the evidence prior to transferring it to another individual. In addition to following these procedures, when transferring to or receiving evidence from another person, I am also sure to properly sign, date, and note the reason for the transfer.

6. With regard to each item of physical evidence I received in this case, I followed these same procedures. When receiving whole computers, I also checked to ensure they did not contain any suspicious hardware or removable data storage devices such as SD cards and thumb drives. Prior to powering on or accessing the contents of any device, I imaged each item of physical evidence I received in order to preserve the contents of the data on the item. A forensic image of an item of digital media is an exact, bit-for-bit copy of the data on the digital media. I imaged these items of evidence so that the data on the device can be forensically examined without manipulating the data contained on the original evidence. This is standard practice by digital forensic examiners. The software forensic examiners use to image the digital evidence has built in procedures to verify that the item has been successfully duplicated. For example, the program will note the MD5 Hash or Secure Hash Algorithm 1 (SHA1) hash value of an item of digital evidence before imaging (acquisition hash value) and after imaging the item (verification hash value). If the two hash values match, the item has been successfully duplicated bit-for-bit. The hash value is determined by mathematical algorithm and is displayed as a number/letter identifier unique to every item of electronically stored information. It is similar to a digital fingerprint,

although more unique. When the hash value is generated, the entire hard drive will have a hash value, as well as each individual file on the hard drive. If there is any alteration to the hard drive or to any file on the hard drive, the acquisition and verification hash values will not match. The alteration can be a small as adding a single space into a text document or saving a file in a different format (i.e. saving a ".doc" as a ".pdf"). In this case, I used EnCase forensic software to complete this imaging process. EnCase forensic software is widely used by digital forensic examiners. As I stated earlier, I have received training on EnCase forensic software and have used it in my other cases involving digital forensic examinations. I encountered no errors while conducting the imaging of the evidence at issue in this case.

7. Between 30 May 2010 and 1 June 2010, I processed the following items of physical evidence:

a. I processed a Hitachi brand laptop computer, with the serial number 070817DP0C10DSG2J1DP, which was collected from the Supply Office or Annex, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This computer was marked "UNCLASSIFIED" and was seized because PFC Manning had temporarily worked in the Supply Office in May 2010 and used this computer. I received this evidence from SA Thomas Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed this computer and obtained an EnCase forensic image of the hard drive contained within this computer. The resulting forensic image, with the SHA1 hash value of 309df99f068fba2e81aae03dla93d471cde90bf0, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. I did not examine this image further. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 1 of DN 073-10. I know this because I collected Item 1 as evidence.

b. I processed a Seagate brand computer hard drive, with the serial number CN-0MN922-21232-793-002L, which was collected from the Supply Office/Annex, 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This computer was connected to the SIPRNET and the hard drive was seized because PFC Manning had temporarily worked in the Supply Office in May 2010 and used this computer. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed this hard drive and obtained an EnCase forensic image of the hard drive. The resulting forensic image, with the SHA1 hash value of cf6d703f0023773e b9e30eeb318660ac0d18f404, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. I did not examine this image further. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 2 of DN 073-10. I know this because I collected Item 2 as evidence.

c. I processed a rewriteable compact disc (CD-RW), with the serial number LD623MJ04184038B16, which was collected from the quarters of PFC Manning, Room 4C93, LSA Dragon, FOB Hammer, Iraq. A CD-RW is different from a commercially-produced CD with content already loaded onto it (i.e. from a music store), because a CD-RW allows the user to write content to the CD, along with edit or delete information on the CD. This CD-RW had a

"SECRET" sticker on it and was labeled "12 Jul 07 CZ ENGAGEMENT ZONE 30 GC". This CD-RW was collected with three Arabic language CDs in a multi-disc case. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the multi-disc case and obtained an EnCase forensic image of the aforementioned CD-RW. The resulting forensic image, with the MD5 hash value of 5c993ee621b036482bae1353f844322f, was verified to be an exact, bit-for-bit copy of the CD-RW through a comparison of the acquisition and verification hash values. After imaging this CD-RW, I conducted a preliminary forensic examination of this image. The CD-RW contained two files with identical names. One file contained no data and the other file, "12 Jul 07 CZ ENGAGEMENT ZONE 30 GC," contained a video. The video appeared to have been burned to the disc on 27 April 2010 using Macintosh disc creation software. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 2 of DN 073-10. I know this because I collected Item 2 as evidence.

d. I processed an Apple brand laptop computer, with the serial number W8939AZ066E, which was collected from the quarters of PFC Manning, Room 4C93, LSA Dragon, FOB Hammer, Iraq. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the Macintosh computer, removed a Fujitsu brand hard drive from the laptop, and obtained an EnCase forensic image of the hard drive. The serial number of the hard drive was K94DT9829WPY. The resulting forensic image of the hard drive I obtained from this computer, with the SHA1 hash value of 3cf107db8b3865a5e3ebfce400bae1da9691fb49, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. Thereafter, I conducted a preliminary forensic examination of this image. I determined that the hard drive had a Macintosh operating system installed and had a user account resembling PFC Manning's name, although I did not note the machine's username in my Agent's Investigation Report (AIR). A review of the device logs contained on the hard drive revealed some form of optical disc (i.e. CD-RW drive) activity occurred, like deleting or burning CD-RWs, on or around 27 April 2010. I also reviewed the "user" files associated with the account resembling PFC Manning's name and located several files containing text that was specifically referenced in the chat logs received by U.S. Army CID during the initial phases of the investigation, though I did not specifically note which text was referenced in the chat logs in my AIR. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 1 of DN 073-10. I know this because I collected Item 1 as evidence.

e. I processed a Seagate brand external hard disk drive (HDD), with the serial number 2GEWJKLJ, which was collected from the quarters of PFC Manning, Room 4C93, LSA Dragon, FOB Hammer, Iraq. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the external HDD case and further removed the internal HDD, also Seagate brand (serial number 9VS1S2TZ), because I did not have a power adapter that could safely and reliably power the Seagate brand external HDD. I then obtained an Encase forensic image of the internal Seagate HDD with the SHA1 hash value of 151183463c5b5841a8115627bf51e8d9e74abb48. The resulting forensic image was verified to be an exact, bit-for-bit copy of the Seagate HDD through a comparison of the acquisition and verification hash values. After imaging the Seagate HDD, I conducted a preliminary forensic examination of this image. I found a file containing the contact information of a member of the WikiLeaks team, Mr. Julian Assange. This contact information appeared to have been produced and released by the WikiLeaks team and did not appear to be of a personal nature. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 1 of DN 073-10. I know this because I collected Item 1 as evidence.

f. I processed an Alienware brand laptop computer, with the serial number NKD900TA6D00661, which was collected from the Sensitive Compartmented Information Facility (SCIF) of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This computer was connected to the SIPRNET and the hard drive was seized because PFC Manning had worked in the SCIF in November 2009 to May 2010 and used this computer. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the Alienware laptop computer, removed the Seagate brand hard drive from the laptop, and obtained an EnCase forensic image of the hard drive. The serial number of the hard drive was 3MH036M1. The resulting forensic image of the hard drive I obtained from this computer, with the SHA1 hash value of c7400fbed0b4db68a582a585eeaa34ab1a62cd64, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. Thereafter, I conducted a preliminary forensic examination of this image. I determined that PFC Manning had a user account on this laptop computer. I found several items of interest to this investigation, including copies of the Apache video made publically available by WikiLeaks and called "Collateral Murder." I also found an archive file that contained approximately 11,000 sensitive and classified documents, downloaded in Hyper Text Markup Language (HTML) format, though I did not note the exact number. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 2 of DN 073-10. I know this because I collected Item 2 as evidence.

g. I processed a Dell brand laptop computer, with the serial number HLVJQF1, which was collected from the Sensitive Compartmented Information Facility (SCIF) of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This computer was connected to the SIPRNET and the hard drive was seized because PFC Manning had worked in the SCIF in November 2009 to May 2010 and used this computer. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the Dell laptop computer, removed an unknown brand hard drive from the laptop, and obtained an EnCase forensic image of the hard drive. The serial number of the hard drive was 5MH0HWKN. The resulting forensic image of the hard drive I obtained from this computer, with the SHA1 hash value of c3473c3df1d131e0022f0c56bfc46087e9d5150f, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. Thereafter, I conducted a preliminary forensic examination of this image. I determined that PFC Manning had a user account on this laptop computer. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 2 of DN 073-10. I know this because I collected Item 2 as evidence.

h. I processed a Dell brand laptop computer, with the serial number 93H4QD1, which was collected from the Sensitive Compartmented Information Facility (SCIF) of the 2nd Brigade Combat Team, 10th Mountain Division, FOB Hammer, Iraq. This NIPRNET laptop had been located near the work area of PFC Manning. I received this evidence from SA Smith. I followed proper evidence handling procedures to receive and handle this evidence, and made sure the evidence matched its noted description before beginning work. Upon taking possession, I unsealed the Dell laptop computer, removed an unknown brand hard drive from the laptop, and obtained an EnCase forensic image of the hard drive. The serial number of the hard drive was 5MH0TB78. The resulting forensic image of the hard drive I obtained from this computer, with the SHA1 hash value of e2b49bd3ed0e2f5d798ab44febaac3b15d0070be, was verified to be an exact, bit-for-bit copy of the hard drive through a comparison of the acquisition and verification hash values. I did not examine this image further. I reviewed DN 073-10 in preparation for this case. This item's forensic image is located on Item 1 of DN 073-10. I know this because I collected Item 1 as evidence.

8. As I stated earlier, I used the EnCase forensic software to obtain the images of each item of evidence I processed. In this case, I attached each device (except the CD-RW) to a write-blocker, and then attached the write-blocker to my laptop computer, which had the EnCase forensic software loaded. A write-blocker is a device that allows you to acquire information on an item of digital media without accidentally damaging or altering the contents of the original item of digital media. In short, the write-blocker ensures that none of the original data on the item of evidence is manipulated in any way. I did not use the write-blocker when processing the CR-RW, as that device was not at risk of alteration. Computers do not alter data on CD-RWs without specific instructions to do so. As I neither intended nor actually issued such instructions, there was no need to use a write-blocker with regards to the CD-RW. After securing the write-blocker as appropriate, I then used EnCase to create a forensic image of each item. As I stated earlier, EnCase creates an acquisition hash value that is later compared to the verification hash value once the image has been created. I saved the forensic images of each device I processed onto sterile hard drives. I later transferred these forensic images to the hard drives recorded as Items 1 and 2 on DN 073-10. The forensic image is not altered by being transferred between storage devices. When you open the forensic image in EnCase, EnCase itself verifies that the forensic image is a true copy.

9. Item 1 of DN 073-10, serial number 9VS25G5M, is a Seagate brand hard disk drive containing the individual forensic images of the devices listed above that were initially determined to be "UNCLASSIFIED." Item 2 of DN 073-10, serial number 5VG1826C, is a Seagate brand hard disk drive containing the individual forensic images of the devices listed above that were initially determined to be classified "SECRET." On 5 June 2010, I collected Items 1 and 2 as evidence because I had previously transferred the forensic images of the various devices I processed to these two hard disk drives. I collected this evidence at the CID office on Camp Liberty. I did this to consolidate the evidence I processed for ease of review by subsequent forensic examiners. This process is consistent with best computer forensic practices. In the forensic community, it is common for investigators to consolidate the forensic images of multiple devices on one hard drive and then collect the resulting hard drive as evidence. After I collected Items 1 and 2 as evidence, I transferred custody of this evidence to SA Jeremy Drews.

10. During the above forensic examinations, I recorded my notes, including descriptions of the evidence and their associated hash values on an AIR, dated 5 June 2010, and marked for this court-martial with bates numbers: 00021674 - 00021683. This AIR accompanied the evidence I transferred to SA Drews.

11. Prosecution Exhibit 11 for Identification is the Seagate brand hard disk drive with serial number 9VS25G5M (Item 1 of DN 073-10). Prosecution Exhibit 12 for Identification is the Seagate brand hard disk drive with serial number 5VG1826C (Item 2 of DN 073-10).

JoDean Morrow
JODEAN MORROW
CPT, JA
Assistant Trial Counsel

Thomas F. Hurley
THOMAS F. HURLEY
MAJ, JA
Defense Counsel

BRADLEY E. MANNING
PFC, USA
Accused